Google Scholar BETA

Web Images Video News Maps **more »**

galois field encryption shift register Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

Scholar **All articles** - Recent articles Results **1** - **10** of about **4,240** for **galois field encryption shift register**. (**0.25** seconds)

[BOOK] Shift Register Sequences
SW Golomb, S Golomb - 1981 - Aegean Park Press Laguna Hills, CA, USA
Cited by 1191 - Related Articles - Web Search

A digital watermark - all 8 versions »
RG van Schyndel, AZ Tirkel, CF Osborne - Image Processing, 1994. Proceedings. ICIP-94., IEEE ..., 1994 - ieeexplore.ieee.org
... Conventional techniques involve the **encryption** of a **...** generated) form a finite **field** called **Galois Field**. **...** order to determine the **shift register** configuration [3 **...**
Cited by 502 - Related Articles - Web Search

Public-key cryptosystems based on cubic finite **field** extensions - all 3 versions »
G Gong, L Harn - Information Theory, IEEE Transactions on, 1999 - ieeexplore.ieee.org
... Index Terms— Characteristic sequence, cubic finite **field** extension, linear feedback **shift-register** sequence, public-key exchange scheme, RSA-type **encryption**. **...**
Cited by 67 - Related Articles - Web Search - BL Direct

Fast Arithmetic for Public-Key Algorithms in **Galois** Fields with Composite Exponents - all 22 versions »
C Paar, P Fleischmann, P Soria-Rodriguez - IEEE TRANSACTIONS ON COMPUTERS, 1999 - doi.ieeecomputersociety.org
... elliptic curves) rely on finite **field** multiplication as **...** polynomial multiplication modulo the **field** polynomial, is **...** is a linear feedback **shift register** (LFSR) of **...**
Cited by 64 - Related Articles - Web Search - BL Direct

A Fast VLSI Multiplier for GF (2 m) - all 3 versions »
P Scott, S Tavares, L Peppard - Selected Areas in Communications, IEEE Journal on, 1986 - ieeexplore.ieee.org
... It is attractive for use in data **encryption** systems where **...** For simplicity, the finite **field** GF(24) is used **...** is transferred to the output **shift register** (OSR) and **...**
Cited by 49 - Related Articles - Web Search

A high speed data **encryption** processor for public key cryptography
T Rosati, CS Inc, O Kanata - Custom Integrated Circuits Conference, 1989., Proceedings of ..., 1989 - ieeexplore.ieee.org
... consists of three 593-bit **shift registers** using systolic **...** to multiply two numbers in the finite **field**. **...** management, authentication, and data **encryption** [7]. In **...**
Cited by 20 - Related Articles - Web Search

Feedback **shift** registers, 2-adic span, and combiners with memory - all 5 versions »
A Klapper, M Goresky - Journal of Cryptology, 1997 - Springer
... These are the **shift register** analogues of the Marsaglia-Zaman pseudorandom **...** different mathematical toolkit: instead of arithmetic in finite **fields**, we use **...**
Cited by 36 - Related Articles - Web Search - BL Direct

An implementation for a fast public-key cryptosystem
GB Agnew, RC Mullin, IM Onyszchuk, SA Vanstone - Journal of Cryptology, 1991 - Springer
... discoveries in the structure of finite **fields** used, provide **...** the RSA system where the **encryption** exponent Ei **... field** which does, there are advantages to choosing **...**
Cited by 111 - Related Articles - Web Search

Pseudo-random sequences and arrays - all 2 versions »

FJ MacWilliams, NJA Sloane - Proceedings of the IEEE, 1976 - ieeexplore.ieee.org
... 1, together with the zero sequence, are isomorphic to a **field** with 2m **...** PSEUDO-RANDOM SEQUENCES A. The **Shift Register** To construct a pseudo-random sequence of **...**
Cited by 220 - Related Articles - Web Search

A High-Performance Reconfigurable Elliptic Curve Processor for GF (2 m) - all 23 versions »
G Orlando, C Paar - Cryptographic Hardware and Embedded Systems—CHES, 2000 - Springer
... private-key algorithms for bulk data **encryption** after that **...** is the hardware that computes the finite **field** operations **...** For the **field** polyno- mials recommended for **...**
Cited by 139 - Related Articles - Web Search - BL Direct

Key authors: **S Golomb** - **R van Schyndel** - **A Tirkel** - **C Osborne** - **C Paar**

Gooooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**